# 基于 LBP 人脸纹理特征的差分直方图移位无损信息隐藏算法 *

张　弢 [1a]，柳雨农 [1a†]，任　帅 [1b]，张德刚 [2]

(1. 长安大学 a. 电子与控制工程学院; b. 信息工程学院，西安 710068; 2. 云南电网有限责任公司 教育培训评价中心，昆明 650033)

**摘　要：**针对信息隐藏算法中提高嵌入量与增强鲁棒性之间的矛盾问题，提出一种多载体信息隐藏算法。使用多幅人脸表情图像作为载体，采用局部二值模式（LBP）纹理特征识别人脸表情区域来嵌入加密信息;计算出载体区域的相邻像素差值矩阵，通过对差值矩阵的对应元素的直方图进行移位构造出嵌入空间来实现加密信息的可逆隐藏与载体图像的无损恢复。算法分析证明了比现有算法具有更大的嵌入容量并保持较高的鲁棒性的优势，在最大嵌入容量达到 0.561 同时具有 38.421 dB 的信噪比（PSNR），且在识别的嵌入区域 PSNR 值达到 46.286。鲁棒性实验表明，该算法对于滤波攻击可以与原始信息图像的相似度大于 99%；面对剪切、平移攻击时，秘密图像归一化系数（NC）最小为 0.743 和 0.728，远大于其他算法。从与其他算法的对比实验结果看，提出的算法是有效的。

**关键词：**无损信息隐藏；多载体；局部二值模式；差分矩阵；直方图移位

**中图分类号：**TP309.2　　doi: 10.19734/j.issn.1001-3695.2018.11.0889

## Differential histogram shift lossless information hiding algorithm based on LBP face texture features

Zhang Tao[1a], Liu Yunong[1a†], Ren Shuai[1b], Zhang Degang[2]

(1. *a. School of Electronic & Control Engineering*, *b. School of Information Engineering*, *Chang'an University*, *Xi'an* 710064, *China*; 2. *Education Training Evaluation Center, Yunnan Power Grid Co*, *Kunming* 650033, *China*)

**Abstract:** Aiming at the contradiction between improving the embedded quantity and enhancing the robustness in the information hiding algorithm, this paper proposed a multi-carrier information hiding algorithm. The algorithm used multiple facial expression images as vectors, and applied local binary pattern (LBP) texture features to recognize facial expression regions to embed encrypted information. Calculating the adjacent pixel difference matrix of the carrier region, and constructing the embedded space by shifting the histogram of the corresponding element of the difference matrix , in order to realize the reversible concealment of the encrypted information and the lossless recovery of the carrier images. Algorithm analysis proves that it has greater embedding capacity and maintains higher robustness than existing algorithms. Its largest embedded capacity reaches 0.561 at same time the peak signal to noise ratio (PSNR) is 38.421dB. And the value of embedded region PSNR in the paper. reaches 46.286. The robustness experiments show that the proposed algorithm may have a similarity greater than 99% to the original information image for the filtering attack. In the face of shear and translation attacks, the minimum image normalization coefficient (NC) is 0.743 and 0.728, which is much larger than other algorithms. From the comparison experimental results with other algorithms, the proposed algorithm is effective.

**Key words:** lossless information hiding; multi-carrier; mocal binary pattern; difference matrix; histogram shift

## 0　引言

随着物联网、大数据、社交网络、虚拟现实等技术的发展，以人类行为以及客观事物描述信息作为载体传输机密信息的技术飞速增长。解决大容量秘密信息与嵌入算法的鲁棒性之间的矛盾已成为研究的主流方向之一，隐藏者不可避免地利用多个载体负载信息的问题归为多载体信息隐藏与联合分析。Ker 研究了载体计数分析、平均联合分析、广义似然率测试 3 种不同策略下的情况[1]，并在载体计数分析中关于阈值选取的博弈均衡进行了研究[2]，证明了多载体安全嵌入容量正比于载体数量的平方根而非载体数量[3]，单载体安全嵌入容量正比于载体大小的平方根[4]，进而给出最小化 KL divergence 的多载体隐藏策略[5]。

针对单载体信息隐藏算法的隐藏容量小、安全性较低的问题，近年来基于多载体的方案，文献[6]中提出了一种基于 Bernstein 多项式的多载体分存隐写算法，为秘密信息的嵌入提供了较大的嵌入空间，但由于分存的载体图像之间存在较强的相关性，只对特定的攻击存在较强的鲁棒性；文献[7，8]提出一种基于误差扩散的多幅图像隐藏方案，利用不相关图像作为载体，将量化误差分散到当前处理点的邻域像素中，得到较好的视觉效果，但提取信息时载体与原图像存在差异，而且当丢失任一分存图可导致秘密信息无法提取，文献[9]

**收稿日期：**2018-11-21；**修回日期：**2019-01-08　**基金项目：**国家自然科学基金资助项目（61702050，61402052）；国家级大学生创新创业训练计划资助项目（201610710036）

**作者简介：**张弢（1984-），女，山西吕梁人，副教授，博士，主要研究方向为多载体信息隐藏技术；柳雨农（1993-），男，甘肃平凉人，硕士研究生，主要研究方向为非常规载体信息隐藏；任帅（1982-），男，山西太原人，副教授，博士，主要研究方向为信息隐藏理论与模型；贺媛（1994-），女，陕西神木人，硕士研究生，主要研究方向为 3D 模型处理与应用；徐振超（1992-），男，山西长治人，硕士研究生，主要研究方向为信息隐藏及数字信息技术；王震（1993-），男，山西运城人，硕士研究生，主要研究方向为多媒体数据检索及认证；慕德俊（1963-），男，山东荣成人，教授，博导，主要研究方向为网络与信息安全.

提出一种基于固定阻塞的多载波分散信息隐藏算法。

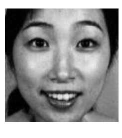
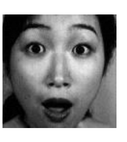
主流的嵌入算法依旧采用单载体隐藏算法，而多载体信息隐藏的优点在于解决了载体嵌入容量与算法鲁棒性之间的矛盾。本文提出了一种新颖的基于局部二值模式（local binary pattern，LBP）人脸表情识别[10]区域的多载体信息隐藏算法。在多幅人脸表情图像中，通过区域块匹配的方法来确定人脸表情特征的运动向量，并使用主成分分析方法(PCA)从这些运动向量中产生低维子空间，即特征运动空间[11]。利用自表情区域框动识别的表情运动特征空间，在特征空间采用差分直方图移位调整像素值来嵌入预处理后的加密信息[12]。实验表明，嵌入加密信息后，由于具有较大嵌入空间，含密表情图像保持原有的人脸表情，并经过剪切、高斯噪声以及旋转等攻击时保持了较好的鲁棒性。使用逆差分直方图移位算法提取加密信息后，得到与原始载体一致的表情图像及信息图像，从而实现了大嵌入容量在多个载体的无损信息隐藏效果。

## 1　人脸表情特征区域识别

多载体信息隐藏技术的计算复杂度相较同类单载体算法有所增加，但有效地解决了嵌入算法提高嵌入容量难的问题[13]。本文在 JAFFE(Japanese female facial expression)人脸表情库中选取 4 幅不同表情图像，表情特征区域提取步骤为:

a)在原始表情图像中调整面部区域，使其大小为 512×512，4 幅表情载体如图 1 表示为 $C_1$、$C_2$、$C_3$、$C_4$。



$C_1$　　$C_2$　　$C_3$　　$C_4$

图 1　调整大小后表情载体图像

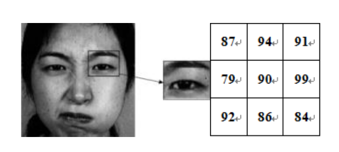
Fig. 1　Image of the emoticon after resizing

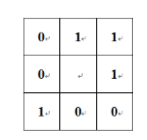
b)通过 LBP 提取表情的纹理特征。选取 3×3 矩阵，根据 LBP 变换式（1），以中心像素值为阈值遍历整幅图像，作如图 2 矩阵变换，得到 LBP 特征纹理，可以清晰地反映出表情局部细节；

$$LBP(x_c, y_c) = \sum_{p=0}^{p-1} 2^p s(i_p - i_c) \tag{1}$$

其中:（$x_c$，$y_c$）为 3×3 矩阵中心像素，$i_p$、$i_c$ 为领域像素，$s(x)$ 为符号函数，定义:

$$s(x) = \begin{cases} 1 & if \quad x \geq 0 \\ 0 & else \end{cases} \tag{2}$$







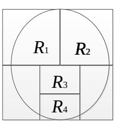
(a)局部区域　(b)区域像素矩阵 (c)LBP 变换矩阵 (d)人脸纹理特征

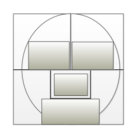
图 2　LBP 人脸表情纹理特征提取

Fig. 2　LBP facial expression texture feature extraction

c)基于步骤 b)的特征纹理图像，进行二值化变换得到谷峰图像（图 3（a）），通过块匹配的方法来确定表情人脸和的运动向量，并用主成分分析法(principal components analysis，PCA)从这些运动向量中产生低维子空间，得到一般特征区域为 $R_1$、$R_2$、$R_3$、$R_4$。

d)在 $R_1$、$R_2$、$R_3$、$R_4$ 中选择重要特征区域作为加密信息的嵌入空间，选择其中最大区域 $R_4$ 作为加密信息的嵌入区域，在图 3(d)中的人脸图像中得到嵌入区域框大小为 225×144。




(a)谷峰图像　(b)一般特征框　(c)主要特征框　(d)信息嵌入区域

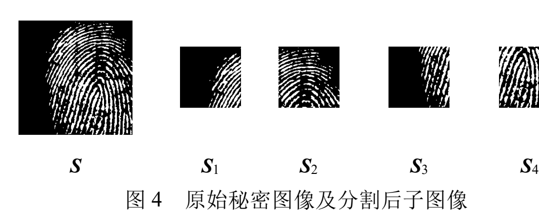
图 3　加密信息嵌入区域选取

Fig. 3　Encrypted information embedding area selection

e)重复步骤 a)~d)，对其他三幅人脸表情图像提取加密信息嵌入区域。

## 2　秘密信息预处理

本次算法中选取某大小为 128×128 的二值指纹图像 $\boldsymbol{S}$ 作为秘密信息，并分割为 4 幅大小相同的子图像 $\boldsymbol{S}_1$、$\boldsymbol{S}_2$、$\boldsymbol{S}_3$、$\boldsymbol{S}_4$。



$\boldsymbol{S}$　$\boldsymbol{S}_1$　$\boldsymbol{S}_2$　$\boldsymbol{S}_3$　$\boldsymbol{S}_4$

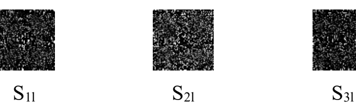
图 4　原始秘密图像及分割后子图像

Fig. 4　Original secret image and segmented sub-image

置乱加密是打乱图像像素顺序，有效地去除像素之间的相关性，使秘密信息在传输过程中更安全。对分割的秘密信息子图像进行 Logistic 映射混沌置乱，在一维 Logistic 映射、超 Logistic 映射基础上，一种量子 Logistic 映射被提出[14]，但非线性动力学特性复杂。为简化算法的计算复杂度，在一维 Logistic 映射迭代式(3)中，设定 Logistic 映射参数 $\mu$=3.99，初始值 $x_0$=0.5 时，在 $n$ 次迭代后得到一个非周期、不收敛的混沌序列，且 $n$ 值越大其置乱效果越高。

$$x_n + 1 = x_n \times \mu(1 - x_n) \tag{3}$$

其中:$\mu \in [0,4]$，$x \in (0,1)$。图 5 为 Logistic 映射混沌置乱后秘密信息子图像 $S_{1l}$、$S_{2l}$、$S_{3l}$、$S_{4l}$，从置乱结果看出，秘密信息已经失去了原来的纹理特征。





$S_{11}$　$S_{21}$　$S_{31}$　$S_{41}$

图 5　秘密信息 Logistic 映射置乱

Fig. 5　Secret information Logistic map scrambling

## 3　嵌入算法

本文基于多载体的思想，Kittawi 等人[15]提出了利用载体图像的直方图移位构造冗余空间，实现隐藏信息的嵌入，但直接使用直方图移位造成冗余空间有限，无法嵌入更多的信息量；文献[16，17]中提出了一种中值差分直方图的可逆数据隐藏，通过修改两个选定区域，保留直方图的中间点来实现隐藏信息的盲提取，并得到了较好的视觉效果。本文基于[16]中算法提出一种差分直方图移位的信息嵌入算法，利用相邻像素的差的直方图构造冗余空间，增大了嵌入空间，以及实现载体图像与秘密信息的无损提取。

### 3.1　计算相邻像素差

定义载体图像 $\boldsymbol{C}\{C_1$、$C_2$、$C_3$、$C_4\}$大小为 $\boldsymbol{M}\times\boldsymbol{N}$ 的 8 位灰度图像，$\boldsymbol{C}(i,j)$为载体图像在$(i,j)$点的像素值，按行依次计算列方向的相邻像素差，表示为

$$D_l(i,j)=C(i,j)-C(i,j+1) \tag{4}$$

其中：$1\le i\le M$，$1\le j\le N-1$。行方向相邻像素差为

$$D_r(i,j)=C(i,j)-C(i+1,j) \tag{5}$$

其中：$1\le i\le M-1$，$1\le j\le N$。图 6 为载体图像 $C_1$、$C_3$ 灰度直方图及像素差值直方图：

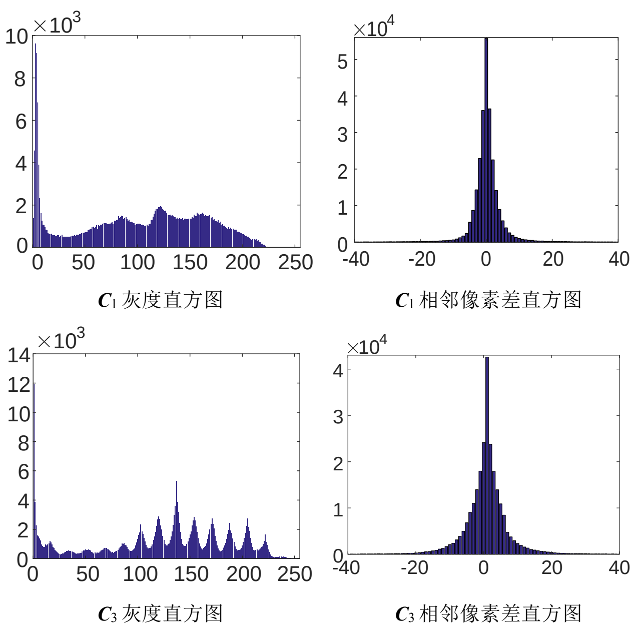



图 6　$C_1$、$C_3$ 灰度直方图及像素差值直方图

*Fig. 6*　$C_1$, $C_3$ gray histogram and pixel difference histogram

图 6 中，载体图像 $C_1$、$C_3$ 相邻像素差分直方图呈拉普拉斯分布，$C_1$ 灰度直方图峰值为 9762，相邻像素差值在"**0**"时的值为 42592；$C_3$ 直方图峰值为 12063，像素差值在"**0**"时的值为 55776，相邻像素差值峰值远大于灰度直方图峰值，可见应在像素相同的相邻像素之间才可构造出更大的冗余空间来嵌入信息。

## 3.2　秘密信息嵌入

可选择按行计算列方向的相邻像素差，亦可按列计算行方向的像素差，为了简化算法复杂度，选择列方向的像素差构造冗余空间，记 $D=D_l$ 为差分矩阵。对差分矩阵 $D$ 进行如图 7 的行调整，构造冗余空间，其中 $\delta$ 为像素差绝对值。

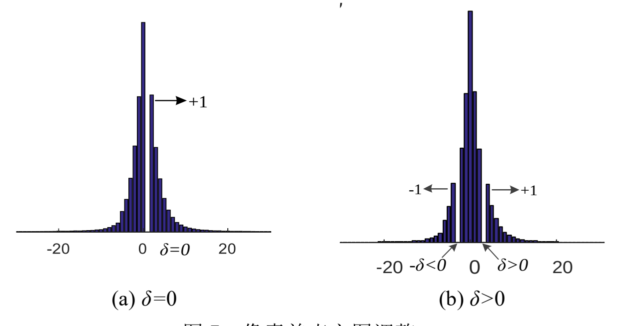



图 7　像素差直方图调整

Fig. 7　Pixel difference histogram adjustment

a）当 $\delta=0$ 时，即载体图像中在像素值相同的相邻像素之间嵌入信息。按光栅顺序扫描差分矩阵 $D$，对各元素作式（6）变换，该变换将消除差值矩阵中值为 1 的元素。

$$D'(i,j)=\begin{cases}D(i,j)+1, & D(i,j)>0\\ D(i,j), & otherwise\end{cases} \tag{6}$$

由于待嵌入加密信息为二进制比特流，嵌入信息比特值记为 $b$，按光栅顺序扫描矩阵 $D'$，使用矩阵中 0 元素按式（7）嵌入比特值 $b$ 嵌入后的像素差值矩阵为 $D''$。当 $b$=0 时，嵌入元素不变，当 $b$=1 时，嵌入元素值加 1。

$$D''(i,j)=\begin{cases}D'(i,j)+1, & D'(i,j)=0\ \&\ b=1\\ D'(i,j), & otherwise\end{cases} \tag{7}$$

b）当 $\delta>0$ 时，即载体图像中相邻像素差值为$\pm\delta$ 的像素嵌入信息。按光栅顺序扫描差分矩阵 $D$，保持在$[-\delta,\delta]$之外的元素不变，只改变在$[-\delta,\delta]$内的元素数值，变换规则如下：

$$D'(i,j)=\begin{cases}D(i,j)+1, & D(i,j)>\delta\\ D(i,j)-1, & D(i,j)<\delta\\ D(i,j), & otherwise\end{cases} \tag{8}$$

在该直方图移位过程中像素差值大于 $\delta$ 的直方图右移（左移）1 位，则在矩阵 $D'$中不存在值为 $\delta\pm1$ 的元素。

基于上述步骤得到调整的相邻像素差值矩阵 $D'$，嵌入加密信息 $b$。按光栅顺序扫描 $D'$，在所有值为$-\delta$-1 和 $\delta$+1 的元素中嵌入 $b$，嵌入信息后的像素差值矩阵为 $D''$，嵌入规则如下：

$$D''(i,j)=\begin{cases}D'(i,j)+1, & D'(i,j)=\delta\ \&\ b=1\\ D'(i,j)-1, & D'(i,j)=-\delta\ \&\ b=1\\ D'(i,j), & otherwise\end{cases} \tag{9}$$

嵌入加密信息后的隐秘图像 $C_S$ 为

$$C_S(i,j)=C(i,j+1)+D''(i,j) \tag{10}$$

其中:$1\le i\le M$，$1\le j\le N-1$。由于差值矩阵大小为 $M\times(N-1)$，而载体图像大小为 $M\times N$，多出的最后一列作为参考像素来提取秘密信息，在嵌入信息前后最后一列像素不发生变化。秘密信息嵌入程序实现流程如图 8 所示。

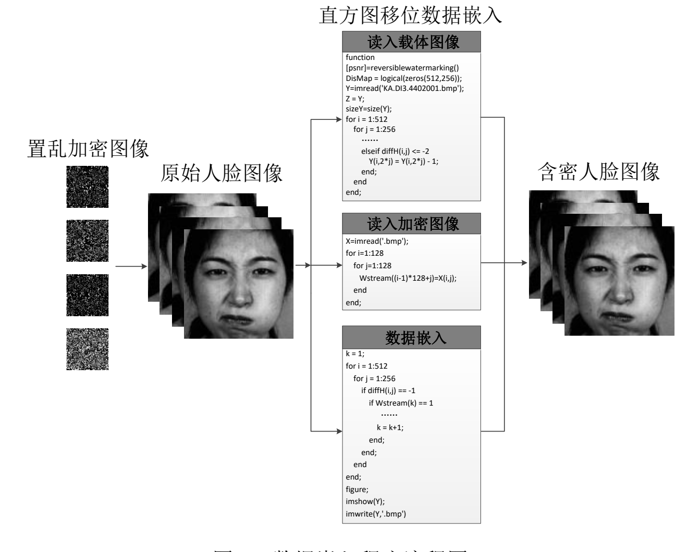



图 8　数据嵌入程序流程图

Fig. 8　Data embedding program flow chart

## 3.3　秘密信息提取

数据的提取和图像恢复为数据嵌入的逆过程。首先对隐秘载体图像从右至左按列方向计算列方向的相邻像素差值矩阵 $D''$，根据提取信息前后最后一列元素不变，$C(i,N)=C_S(i,N)$ 且 $i\in[1,M]$，依 $C(i,N)$计算相邻像素差矩阵 $D''$；

$$D''(i,j)=C_S(i,j)-C(i,j+1) \tag{11}$$

其中：$1\le i\le M$，$1\le j\le N-1$。根据相邻像素差值的绝对值 $\delta$ 的

取值，分为 $\delta=0$ 及 $\delta>0$ 两种情况下恢复载体图像差值矩阵 $\boldsymbol{D}$；

a)当 $\delta=0$ 时，在相邻像素差为 0 的像素嵌入信息情况下。按光栅顺序扫描 $\boldsymbol{D}''$，若扫描元素值为 0，则提取隐藏信息值“0”；当扫描元素为 1 时，提取隐藏信息的值为“1”，并将该元素值置零；当扫描元素大于 1 时，该元素值减 1；则载体图像像素差值矩阵恢复如下：

$$\boldsymbol{D}(i,j)=\begin{cases}\boldsymbol{D}''(i,j)-1, & \boldsymbol{D}''(i,j)>0\\ \boldsymbol{D}''(i,j), & otherwise\end{cases} \tag{12}$$

b）当 δ>0 时，对使用像素差值为-$\delta$ 及 $\delta$ 的像素嵌入的信息进行提取。按光栅顺序扫描 $\boldsymbol{D}''$,若 $\boldsymbol{D}''$ 矩阵中元素值为-$\delta$ 或 $\delta$，提取嵌入信息“0”，$\boldsymbol{D}''$ 矩阵中元素值为-$\delta$-1 或 $\delta$+1 时，提取嵌入信息“1”，并将对应元素值减 1 或加 1；若元素值大于 $\delta$+1 或小于-$\delta$-1 时，对应元素值减 1 或加 1。则提取规则如下：

$$\boldsymbol{D}(i,j)=\begin{cases}\boldsymbol{D}''(i,j)-1, & \boldsymbol{D}''(i,j)\ge\delta+1\\ \boldsymbol{D}''(i,j)+1, & \boldsymbol{D}''(i,j)\le-(\delta+1)\\ \boldsymbol{D}''(i,j), & -\delta\le\boldsymbol{D}''(i,j)\le\delta\end{cases} \tag{13}$$

根据得出的相邻像素的差值矩阵恢复出载体图像 $\boldsymbol{C}'$，即

$$\boldsymbol{C}'=\boldsymbol{C}_S(i,j+1)+\boldsymbol{D}(i,j) \tag{14}$$

其中:1≤$\boldsymbol{i}$≤$\boldsymbol{M}$，1≤$\boldsymbol{j}$≤$\boldsymbol{N}$-1。

秘密信息嵌入的过程是对部分像素值进行 $\boldsymbol{C}(i,j)$+1 或 $\boldsymbol{C}(i,j)$-1 操作，必定会出现部分像素值为 $\boldsymbol{C}(i,j)$<0 或 $\boldsymbol{C}(i,j)$>255 的下溢或上溢情况。因此规定当 $\boldsymbol{C}(i,j)$<0 时的像素值为 0，当 $\boldsymbol{C}(i,j)$<0 时的像素值为 255，以此来解决上溢、下溢问题。秘密信息提取程序实现流程如图 9 所示。

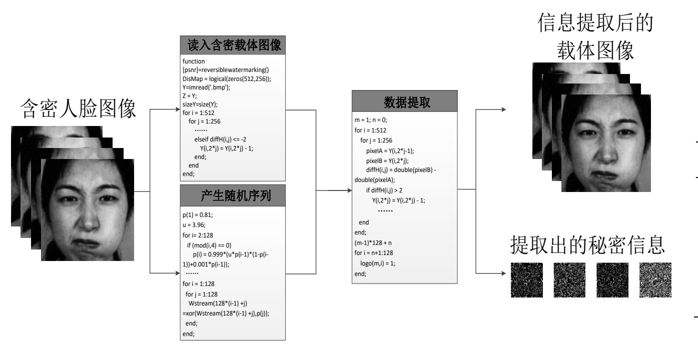



图 9　数据提取程序流程图

Fig. 9　Data extraction program flow chart

### 3.4　嵌入算法实验

在对人脸表情载体图像 $\boldsymbol{C}\{\boldsymbol{C}_1、\boldsymbol{C}_2、\boldsymbol{C}_3、\boldsymbol{C}_4\}$中，通过 LBP 纹理特征提取的嘴部大小为 225×144 的表情区域，根据 3.1 节嵌入步骤嵌入 Logistic 映射置乱的加密信息 $\boldsymbol{S}_l\{\boldsymbol{S}_{1l}、\boldsymbol{S}_{2l}、\boldsymbol{S}_{3l}、\boldsymbol{S}_{4l}\}$，得到隐秘载体 $\boldsymbol{C}_S\{\boldsymbol{C}_{S1}、\boldsymbol{C}_{S2}、\boldsymbol{C}_{S3}、\boldsymbol{C}_{S4}\}$；对隐秘载体进行 3.3 步骤恢复出秘密信息 $\boldsymbol{C}'\{\boldsymbol{C}_1'、\boldsymbol{C}_2'、\boldsymbol{C}_3'、\boldsymbol{C}_4'\}$以及载体图像 $\boldsymbol{S}'\{\boldsymbol{S}_1'、\boldsymbol{S}_2'、\boldsymbol{S}_3'、\boldsymbol{S}_4'\}$。对比得出通过差分直方图移位嵌入算法嵌入信息后，不改变载体图像的纹理特征，由于嵌入区域为表情特征运动能量较大区域，不改变人脸表情。采用逆差分直方图移位对加密信息进行提取，得到无损的载体表情图像，并经过反置乱变换恢复出可识别秘密信息。

峰值信噪比（PSNR）是测量原始图像与隐秘图像之间失真值的一个定量指标，PSNR 的大小反映了秘密图像的嵌入质量，图 11 检测了载体图像 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$、$\boldsymbol{C}_3$、$\boldsymbol{C}_4$ 嵌入容量与 PSNR 之间的关系。差分直方图移位嵌入算法构造了较大的嵌入空间，在设定的表情区域，载体 $\boldsymbol{C}_3$ 嵌入容量最大达到 0.563 时，PSNR($\boldsymbol{C}_3$)$_{max}$=46.286，具有很好的嵌入效果以及不可见性。但载体的嵌入容量的最大必然会降低鲁棒性，图 11 中随有效嵌入容量增大，PSNR 减小，且 PSNR($\boldsymbol{C}_1$)$_{min}$=36.485。表 1 数据中得到平均最大嵌入容量及对应的 PSNR 值为 0.557/37.403，平均最大嵌入容量及对应的 PSNR 值为 0.122/45.823，从数据分析可得出在嵌入容量达到 0.55 时峰值信噪比仍达到 37，表现出含密载体图像与原始表情图像具有很高的相似度。

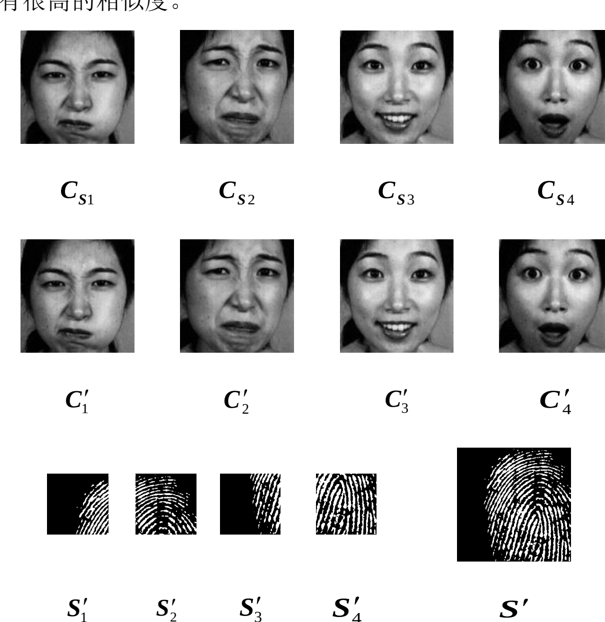



图 10　秘密信息嵌入及恢复

Fig. 10　Secret information embedding and recovery

表 1　载体图像失真检测

Table 1　Carrier image distortion detection

| 载体图像 | $C_1$ | $C_2$ | $C_3$ | $C_4$ |
|---|---|---|---|---|
| 最大容量(dpp) | 0.554 | 0.549 | 0.564 | 0.561 |
| 最小容量(dpp) | 0.126 | 0.122 | 0.118 | 0.121 |
| PSNR(*max*)/dB | 36.485 | 37.382 | 37.323 | 38.421 |
| PSNR(*min*)/dB | 46.286 | 45.706 | 45.569 | 45.741 |

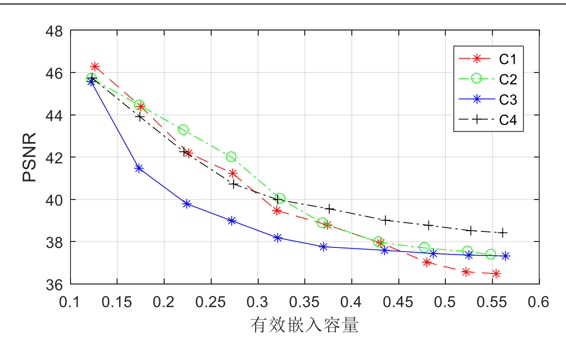



图 11　嵌入容量对鲁棒性的影响

Fig. 11　The effect of embedded capacity on robustness

通过对参考文献算法性能与本文算法进行比较，选取 512×512 的两幅载体图像，对比看出，Yang 等人算法采用了中值差分直方图移位方法，构造出了较高的嵌入空间，并且嵌入容量最大为 0.214，PSNR*max*=49.532；而本文算法同样采用差分直方图移位方法嵌入秘密信息，当嵌入容量大于 0.318 时，PSNR 值高于其他算法，且随着嵌入容量增大，图像的失真度变化较缓，鲁棒性优于其他算法。Wu 等人采用

图像分存算法，由于载体图像之间相关性大，嵌入载体后的图像失真较大，且 PSNR$max$=24.719。

表 2 算法性能比较

Table 2 Algorithm performance comparison

| 载体图像 | 载体 1 | | 载体 2 | |
|---|---|---|---|---|
| | PSNR/dB | 嵌入量 | PSNR/dB | 嵌入量 |
| 本文算法 | 46.286 | 0.126 | 45.569 | 0.118 |
| Cheng 等人算法 | 39.397 | 0.015 | 37.765 | 0.021 |
| Wu 等人算法 | 24.719 | 0.112 | 28.257 | 0.110 |
| Kittawi 算法 | 42.961 | 0.078 | 42.995 | 0.075 |
| Yang 等人算法 | 49.532 | 0.214 | 48.792 | 0.122 |

## 4 鲁棒性实验

检验算法鲁棒性的主要方式为图像进行空间滤波、有损压缩、几何变形等非授权嵌入攻击[18]，检验提取出秘密信息的恢复程度，用提取出秘密信息与原始信息的归一化相关系数作为评估算法鲁棒性的标准，表示如下：

$$NC=\frac{\sum_{i}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i}^{N} w_i^2}\sqrt{\sum_{i}^{N} \hat{w}_i^2}}\begin{cases}\geq T,\text{存在秘密信息}w\\ \leq T,\text{不存在秘密信息}w\end{cases} \quad (15)$$

其中：$w_i$、$\hat{w}_i$ 为秘密信息原始图像及提取后的像素点，$T$ 为预先设定的阈值，经实验，$T$ 值为 0.6 时提取出的秘密信息可识别。

### 4.1 空间滤波鲁棒性实验

对隐秘载体图像 $C_S\{C_{S1}$、$C_{S2}$、$C_{S3}$、$C_{S4}\}$进行均值滤波、高斯滤波、拉普拉斯滤波、高斯-拉普拉斯滤波、中值滤波以及加高斯噪声攻击，提取出加密信息并且复原，其中载体 $C_{S1}$ 滤波攻击的 $NC$ 值如表 3 所示。



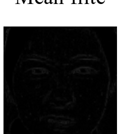
$NC$=0.9987 均值滤波 Mean filte



$NC$=0.9988 高斯滤波 Gaussian filter

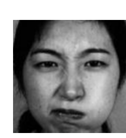


$NC$=0.9992 拉普拉斯滤波 Laplace filter





$NC$=0.9993 高斯-拉普拉斯 Gaussian-Laplace filter





$NC$=0.9986 中值滤波 Median filter



$NC$=0.9985 加高斯噪声 Add Gaussian noise

图 12 $C_{S1}$ 空间滤波攻击

Fig. 12 CS1 Spatial filtering attack

表 3 载体 $C_{S1}$ 在空间滤波攻击下的 NC 值

Table 3 The NC value of carrier $C_{S1}$ under spatial filtering attack

| 滤波攻击 | 均值滤波 | 高斯滤波 | 拉普拉斯滤波 | 高斯-拉普拉斯滤波 | 中值滤波 | 高斯噪声 |
|---|---|---|---|---|---|---|
| 加密信息 $S_1$ | 0.9987 | 0.9988 | 0.9992 | 0.9993 | 0.9986 | 0.9985 |
| 加密信息 $S_2$ | 0.9985 | 0.9989 | 0.9991 | 0.9988 | 0.9987 | 0.9989 |
| 加密信息 $S_3$ | 0.9986 | 0.9993 | 0.9994 | 0.9995 | 0.9978 | 0.9991 |
| 加密信息 $S_4$ | 0.9987 | 0.9987 | 0.9981 | 0.9979 | 0.9988 | 0.9994 |
| 平均 $NC$ 值 | 0.9986 | 0.9989 | 0.9990 | 0.9989 | 0.9985 | 0.9990 |

表 3 中的空间滤波攻击的检测实验结果得出，经过预处理秘密信息，在受到空间滤波攻击后的 $NC$ 值仍大于 0.99，远大于设定的 $NC$ 阈值 0.6。当面临拉普拉斯滤波、高斯噪声攻击时，可获得最大的 $NC$ 值 0.9990，可见当受到空间滤波攻击时，提取出的加密信息恢复后与原始信息具有 99%的相似度，因此表现出很好的抵抗空间滤波攻击性能。

### 4.2 抗几何攻击鲁棒性实验

对隐秘载体图像 $C_S$ 进行平移、剪切、图像缩放几何攻击，提取出加密信息计算 $NC$ 值，求 $NC_S$ 平均值，即 $\overline{NC_S}=\frac{1}{4}\sum_{1}^{4}NC_{Sk}$，表 4~6 为平移、剪切及缩放攻击 $NC$ 平均值，图 13~15 为算法面临攻击时鲁棒性实验。

表 4 平移攻击的 NC 均值

Table 4 NC mean of translational attack

| 平移量 | $NC$ 值 | 平移量 | $NC$ 值 | 平移量 | $NC$ 值 |
|---|---|---|---|---|---|
| 50 | 0.971 | 250 | 0.801 | 450 | 0.748 |
| 100 | 0.905 | 300 | 0.782 | 500 | 0.743 |
| 150 | 0.868 | 350 | 0.765 | | |
| 200 | 0.823 | 400 | 0.753 | | |

表 5 剪切攻击的 NC 均值

Table 5 NC mean of shear attack

| 剪切度/% | $NC$ 值 | 剪切度/% | $NC$ 值 | 剪切度/% | $NC$ 值 |
|---|---|---|---|---|---|
| 5 | 0.991 | 25 | 0.815 | 45 | 0.734 |
| 10 | 0.955 | 30 | 0.776 | 50 | 0.728 |
| 15 | 0.908 | 35 | 0.755 | | |
| 20 | 0.863 | 40 | 0.748 | | |

表 6 缩放攻击的 NC 均值

Table 6 NC Mean of Scaling Attacks

| 缩放倍数 | $NC$ 值 | 缩放率 | $NC$ 值 | 缩放率 | $NC$ 值 |
|---|---|---|---|---|---|
| 0.2 | 0.691 | 1 | 1 | 6 | 0.951 |
| 0.4 | 0.745 | 2 | 0.954 | 8 | 0.958 |
| 0.6 | 0.822 | 4 | 0.957 | | |
| 0.8 | 0.917 | 5 | 0.966 | | |

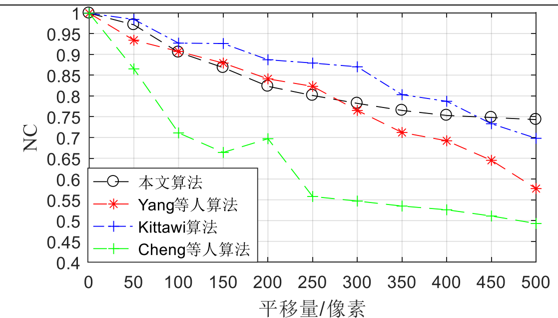



图 13 平移攻击算法性能实验

Fig. 13 Translational attack algorithm performance experiment

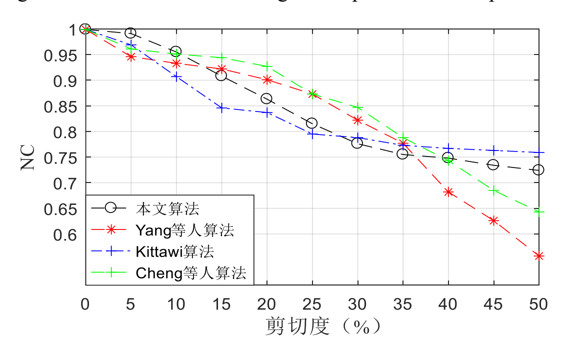



图 14 剪切攻击算法性能实验

Fig. 14 Shear attack algorithm performance experiment

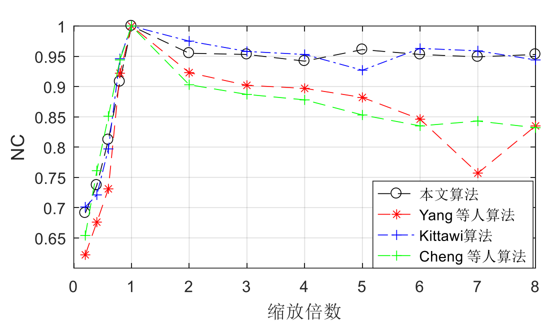



图 15 缩放攻击算法性能实验

Fig. 15 Scaling attack algorithm performance experiment

抗几何变形攻击的鲁棒性实验，表 4 中当平移量=500 时，提取的秘密信息 $NC$ 值为 0.698；表 5 中当剪切度=50%时，提取的秘密信息 $NC$=0.728；表 6 中载体图像缩放比为 0.2 时，$NC_{min}$=0.691，且 $NC_{min}$>0.6，因此秘密信息提取出的保持了较高的可辨识度，几何攻击对秘密破坏较小。对算法性能进行对比，图 13 中 Kittawi 等人算法对平移攻击具有较高的鲁棒性，当平移量>405 时，本文算法抗平移攻击由于 Kittawi 算法；图 14 剪切攻击鲁棒性对比中，当剪切度<28.5%时，本文算法抗剪切性能比 Kittawi 算法性能好，但相比 Cheng 等人算法较弱，剪切度>40%时，本文算法抗剪切性能尤于其他算法。通过数据分析可知，本文算法的抗几何攻击的鲁棒性具有较好的优势，提取的信息保持很高的可识别度。

## 5 结束语

本文提出了一种基于 LBP 人脸纹理特征域的差分直方图移位的多载体无损信息隐藏算法，采用 LBP 纹理特征提取识别出人脸嘴部表情区域，秘密信息为原始秘密图像分割成 4 幅大小相同的子图像，并经过 Logistic 映射混沌置乱进行加密。在选取的大小固定的表情区域，通过计算载体图像相邻像素差得出差值矩阵，根据算法规则调整矩阵直方图来构造出嵌入空间，进行嵌入二值化的加密信息，并经算法逆过程无损提取秘密信息以及恢复载体图像。实验表明，算法使用多载体嵌入信息，嵌入量达到 0.561 的同时保持了 38.421 的 PSNR 值，解决了单幅图像嵌入容量有限的问题。鲁棒性实验中，本文采用差分直方图移位嵌入算法有效地抵抗空间滤波、几何变形等攻击，算法性能对比显示本算法的抗攻击性和鲁棒性较其他算法具有明显的优势。

## 参考文献：

[1] Ker A D. Batch steganography and pooled steganalysis [C]// Proc of the 8th Information Hiding Workshop.2006: 265-281.

[2] Ker A D. Batch steganography and the threshold game [C]// Proc of SPIE:Security, Steganography, and Watermarking of Multimedia Contents. 2007: 401-413.

[3] Ker A D. A capacity result for batch steganography [J]. IEEE Signal Processing Letters, 2007, 14(8): 525-528.

[4] Filler T, Ker A D, Friderich J. The square root law of steganographic capacity for markov covers [C]// Proc of SPIE:Security, Steganography, and Watermarking of Multimedia Contents.2009: 18-22.

[5] Ker A D. Steganographic strategies for a square distortion function [C]// Proc of SPIE:Security, Steganography, and Watermarking of Multimedia Contents.2008: 681904. 1-13.

[6] 陈够喜，沈红雷，伍玉良,等.多载体图像分存隐写算法研究[J]. 计算机工程, 2012, 38(4): 116-118. (Chen Gouxi, Shen Honglei, Wu Yuliang, *et al.* Research on multi-carrier image separation and steganography algorithm [J]. Computer Engineering, 2012, 38(4): 116-118. )

[7] 吴小天，孙伟. 基于误差扩散的图像分存方案 [J]. 计算机应用, 2011, 31(1): 74-77+81. (Wu Xiaotian, Sun Wei. Image sharing scheme based on error diffusion [J]. Journal of Computer Applications, 2011, 31(1): 74-77+81. )

[8] 欧锻灏，吴小天，程斌宜，等. 基于翻转操作的 (2,n) 异或图像分存方案 [J]. 图学学报, 2015, 36(1): 56-61. (Wu Xiaotian, Ou Zhengying, Cheng Binyi, et al. (2,n) XOR image separation scheme based on flip operation [J]. Journal of Graphics, 2015, 36(1): 56-61)

[9] Liang Wei, Jiang Yan, Peng Li, *et al.* A fixed blocking based dispersed information hiding algorithm for multiple carriers [J]. Journal of Computational & Theoretical Nanoscience, 2015, 12(10): 3722-3726.

[10] Guo Hefei, Liu Jianfeng, Dong Zhongwen. Face recognition method based on improved LBP algorithm [J]. Modern Electronics Technique, 2015.

[11] 彭思江，戴厚平，周成富，等. 基于 HOG/PCA/SVM 的跨年龄人脸识别算法 [J]. 吉首大学学报:自然科学版, 2018, 39(5): 24-28. (Peng Sijiang, Dai Houping, Zhou Chengfu, *et al.* An inter-age face recognition algorithm based on HOG/PCA//SVM [J]. Journal of Jishou University & Natural Science Edition, 2018, 39(5): 24-28. )

[12] 郑淑丽，邢慧芬，王美玲，等. 基于直方图平移和差分直方图的可逆水印 [J]. 系统仿真学报, 2013, 25(11): 2717-2722. (Zheng Shuli, Xing Huifen, Wang Meiling, *et al.* Reversible watermarking based on histogram translation and differential histogram [J]. Journal of System Simulation, 2013, 25(11): 2717-2722. )

[13] Elshoura S M, Megherbi D B. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments [M]. Elsevier Science Inc., 2013: 531–552.

[14] 罗玉玲，杜明辉. 基于量子 Logistic 映射的小波域图像加密算法 [J]. 华南理工大学学报:自然科学版,2013, 41(6):53-62. (Luo Yuling, Du Minghui. Image encryption algorithm based on quantum Logistic map in wavelet domain [J]. Journal of South China University of Technology & Natural Science Edition, 2013, 41(6): 53-62. )

[15] KittawiI N, Al-Haj A. Reversible data hiding in encrypted images [C]//Proc of International Conference on Information Technology. Piscataway,NJ:IEEE Press, 2017: 808-813.

[16] Yang H W, Liao I, Chen C C. Reversible data hiding based on median difference histogram. [J]. Journal of Information Science & Engineering, 2011, 27(2): 577-593.

[17] Liu, Li, Chang, Chinchen, Wang Anhong. Reversible data hiding scheme based on histogram shifting ofn-bit planes [J]. Multimedia Tools and Applications, 2016, 75(18): 11311-11326.

[18] Maloo S, Laskshmi N, Pareek N K. Study of digital watermarking techniques for against security attacks [M]// Information and Communication Technology for Intelligent Systems.2018: 509-515.